DEPARTMENT OF THE NAVY

COMMANDING OFFICER
NAVAL AIR STATION
700 AVENGER AVENUE
LEMOORE, CALIFORNIA 93246-5001

NASLEMINST 5239.1F
20
12 MAR 1996

NAS LEMOORE INSTRUCTION 5239.1F

From: Commanding Officer, Naval Air Station, Lemoore

Subj: AUTOMATED INFORMATION SYSTEMS (AIS) SECURITY PROGRAM

Ref: (a) OPNAVINST 5239.1A
(b) SECNAVINST 5239.3
(c) NAVSO P-5239-01
(d) NAVSO P-5239-10
(e) NAVSO P-5239-15
(f) NAVSO P-5239-26
(g) NAVSO P-5239-29
(h) NAS Lemoore Activity Automated Information Security Plan (AAISP)
(i) OPNAVINST 5510.1H
(j) OPNAVINST 5530.14B
(k) OPNAVINST C5510.93
(l) SECNAVINST 5211.5
(m) SECNAVINST 5231.1C

Encl: (1) NAS Lemoore ADP Security Organizational Chart
(2) Automated Information Systems Security Checklist

1. Purpose. To establish the Automated Information Security (AIS) Program required by references (a) and (b). It also serves to encourage all personnel aboard the Naval Air Station Lemoore to actively participate and engage in consistent AIS Security practices.

2. Cancellation. NASLEMINST 5239.1E. This is a major revision, and changes are not annotated in the margins.

3. Background. The Navy has become increasingly dependent upon the use of computers as an aid to mission accomplishment. Desktop computers offer a great variety of applications, therefore they attract a large number of users. Due to ease of access, this equipment has the inherent inability to differentiate between an authorized and unauthorized user. Additionally, the size and portability of the floppy diskette commonly used with these systems incur information security risks not present when only typewriters were used to prepare classified and/or sensitive documents. Use of Local Area Networks (LANs) and Wide Area Networks (WANs) to access other computer systems all over the world compounds the security issue. Therefore, the need to provide protection and security for the Navy's computer systems has become critical.

4. Scope

a. This instruction applies to all AIS systems and networks operated and maintained by NAS Lemoore.

b. The scope of AIS security covers more than just the traditional bounds of security of classified information. It must safeguard all data including but not limited to Privacy Act Data, sensitive financial information, For Official Use Only and the ability to process this data.

5. Objectives

a. NAS Lemoore has a large investment in AIS hardware and software as well as irreplaceable data. AIS security is everyone's responsibility and the Commanding Officer will ensure that it receives the full support required to make the program a success.

b. The AIS Security Program will protect all AIS assets against unauthorized accidental or deliberate modification, disclosure and destruction of data and denial of service to users.

6. AIS Security Organization. Enclosure (1) depicts the AIS Security organizational structure.

7. Duties and Responsibilities. An AIS Security Staff has been appointed to assist in the implementation and administration of the AIS Security Program. Each of these appointments are designated in writing, and will be kept on file until the member is superseded by another. Specific and detailed responsibilities for AIS Security are outlined in reference (a), (b), and (h).

a. Commanding Officer (CO). The CO is responsible for the overall implementation and compliance of the Department of the Navy's (DONs) AIS Security Program, with the following major responsibilities:

(1) Act as the Designated Approving Authority (DAA) for all AISs within the command.

(2) Implement the general administrative, lifecycle management, physical, personnel and information security standards set forth in references (a) thru (m) for protecting AIS equipment, software, data, and facilities from theft, damage, destruction, unauthorized access, disclosure, manipulation, or modification.

(3) Appoint an ADP Security Officer (ADPSO) in writing, to act as the focal point for all AIS security matters, and assistants as required.

(4) Appoint a Responsible Officer in writing, to act as the focal point for all software licensing and copyrighted computer software programs.

b. ADP Security Officer (ADPSO). Reports directly to the Commanding Officer and is responsible for the following major duties:

(1) Act as the focal point and overall manager of the AIS Security Program.

(2) Develops, implements and maintains, Activity Automated Information Systems Security Plan (AAISSP).

(3) Implements a Risk Management and Contingency Plan Program.

(4) Completes accreditation of AISs as prescribed in reference (a), (b) and (d).

(5) Appoints security staff members and assist in implementing their respective AIS security responsibilities.

(6) Ensure procurement documentation comply with established requirements prior to final approval.

(7) Ensure Life Cycle Management (LCM) documentation addresses applicable security requirements per reference (m).

(8) Investigate, document, and report all AIS Security related incidents/violations as prescribed in reference (a).

c. Department ADP Security Officer (DADPSO). Due to the scope of NAS Lemoore's AIS Security Program, DADPSOs will be assigned in writing for each department to assist the ADPSO as needed. Responsibilities are outlined and defined in references (a) and (d).

d. Network Security Officer (NSO). An NSO will be appointed for each LAN for which NAS Lemoore is the sponsor and for the WAN. The NSOs responsibilities include but are not limited to:

(1) Developing, implementing and managing an AIS Security Standard Operating Procedures (SOPs) governing the use of network operations.

(2) Ensure that SOPs are utilized by users at each terminal/workstation accessing the LAN/WAN to maintain integrity of the network.

(3) Develop and implement countermeasures to lower the presence or occurrence of potential risk to the network.

e. Other AIS Security Staff. Responsibilities are outlined and defined in reference (a) and (d).

f. Responsible Officer (RO). ADPSO is assigned the duties of the RO.

(1) Develop, establish, implement and maintain a process and procedure for controlling the use of copyrighted computer software.

(2) Ensure that annual reviews are conducted for evaluation of how the processes and procedures are meeting their goals. Take action to correct any deficiencies discovered.

(3) Monitor the organization's implementation of these procedures.

8. Minimum Program Requirements

a. Enclosure (2) of reference (b) contains the description of the minimum program requirements.

b. In addition to the minimum requirements there are other components of an overall AIS Security Program. These are information, communications, personnel, physical, emanations, software licensing and copyright laws and network security. Each of these elements are managed by different DON programs, but each places certain requirements on NAS Lemoore, which are to be incorporated into the AIS Security Program.

9. Action

a. ADPSO. Conduct security training for newly designated DADPSOs on a quarterly basis. Maintain a master inventory list of all AIS resources. Implement Controlled Access Protection for all computer systems following the guidelines established in references (b) and (c).

b. Department Heads. Assign an DADPSO and if appropriate an ADPSSO for each system within the department. The DADPSO and ADPSSOs must be knowledgeable in microcomputer operations. Ensure a safe and secure AIS computing environment is maintained through the use of enclosure (2).

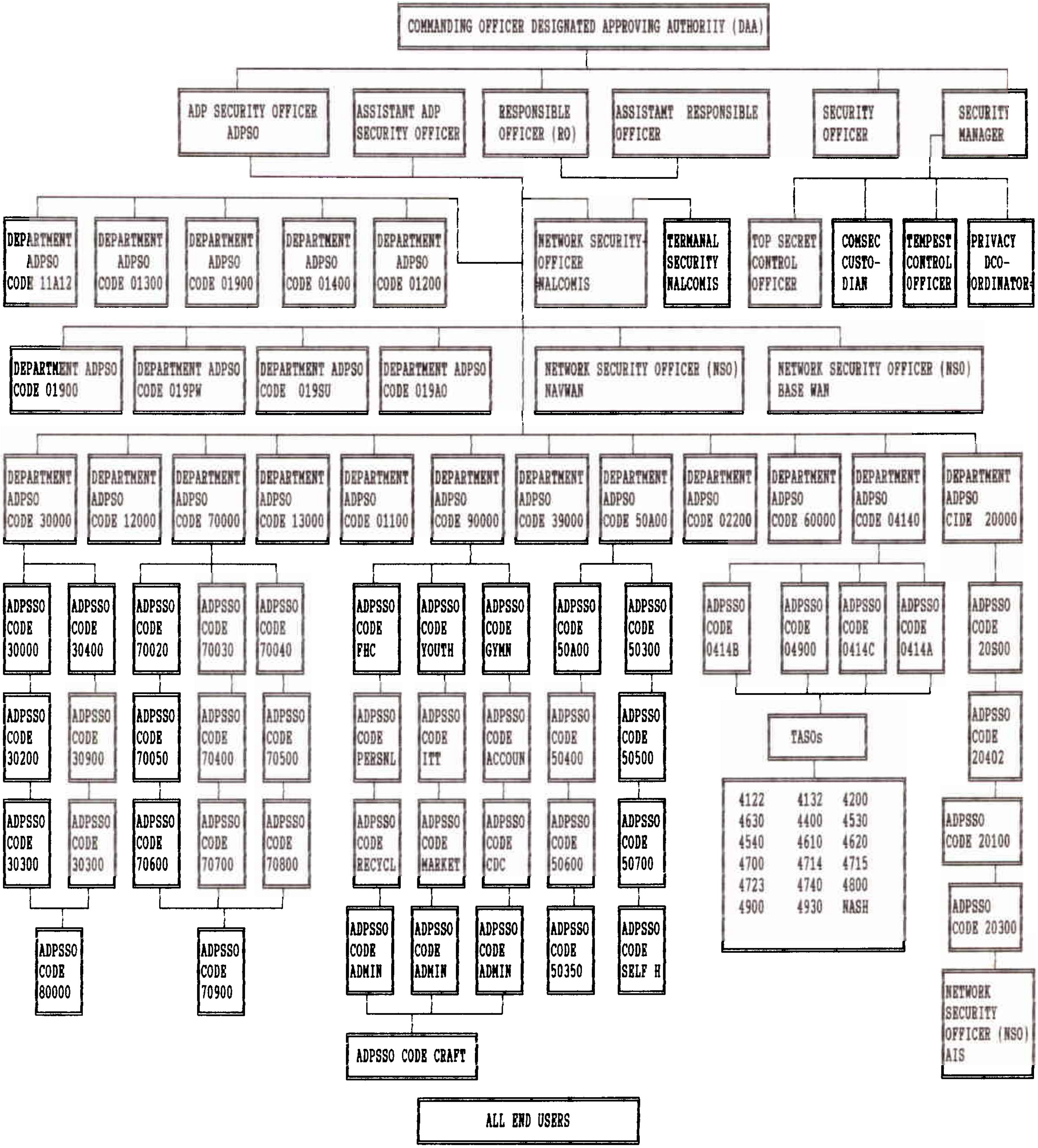
c. DADPSO and ADPSSOs. Enact and enforce microcomputer SOPs and review with all the users quarterly.

d. Responsible Officer. Enact and enforce software licensing and copyrighted computer software program procedures using reference (g) as a guideline.

d. Users. Familiarize yourself with all established SOPs prior to the access and use of any AIS hardware and software. Knowledge and self discipline are the keys to an effective AIS security environment.

GC Wooldridge
G. C. WOOLDRIDGE

Distribution: (NASLEMINST 5215.2U)
Lists B


COMMANDING OFFICER DESIGNATED APPROVING AUTHORITY (DAA)
ADP SECURITY OFFICER ADPSO
ASSISTANT ADP SECURITY OFFICER
RESPONSIBLE OFFICER (RO)
ASSISTAMT RESPONSIBLE OFFICER
SECURITY OFFICER
SECURITY MANAGER
DEPARTMENT ADPSO CODE 11A12
DEPARTMENT ADPSO CODE 01300
DEPARTMENT ADPSO CODE 01900
DEPARTMENT ADPSO CODE 01400
DEPARTMENT ADPSO CODE 01200
NETWORK SECURITY OFFICER NALCOMIS
TERMANAL SECURITY NALCOMIS
TOP SECRET CONTROL OFFICER
COMSEC CUSTO-DIAN
TEMPEST CONTROL OFFICER
PRIVACY DCO-ORDINATOR
DEPARTMENT ADPSO CODE 01900
DEPARTMENT ADPSO CODE 019PW
DEPARTMENT ADPSO CODE 019SU
DEPARTMENT ADPSO CODE 019A0
NETWORK SECURITY OFFICER (NSO) NAVWAN
NETWORK SECURITY OFFICER (NSO) BASE WAN
DEPARTMENT ADPSO CODE 30000
DEPARTMENT ADPSO CODE 12000
DEPARTMENT ADPSO CODE 70000
DEPARTMENT ADPSO CODE 13000
DEPARTMENT ADPSO CODE 01100
DEPARTMENT ADPSO CODE 90000
DEPARTMENT ADPSO CODE 39000
DEPARTMENT ADPSO CODE 50A00
DEPARTMENT ADPSO CODE 02200
DEPARTMENT ADPSO CODE 60000
DEPARTMENT ADPSO CODE 04140
DEPARTMENT ADPSO CIDE 20000
ADPSSO CODE 30000
ADPSSO CODE 30400
ADPSSO CODE 70020
ADPSSO CODE 70030
ADPSSO CODE 70040
ADPSSO CODE FHC
ADPSSO CODE YOUTH
ADPSSO CODE GYMN
ADPSSO CODE 50A00
ADPSSO CODE 50300
ADPSSO CODE 0414B
ADPSSO CODE 04900
ADPSSO CODE 0414C
ADPSSO CODE 0414A
ADPSSO CODE 20S00
ADPSSO CODE 30200
ADPSSO CODE 30900
ADPSSO CODE 70050
ADPSSO CODE 70400
ADPSSO CODE 70500
ADPSSO CODE PERSNL
ADPSSO CODE ITT
ADPSSO CODE ACCOUN
ADPSSO CODE 50400
ADPSSO CODE 50500
TASOs
ADPSSO CODE 20402
ADPSSO CODE 30300
ADPSSO CODE 30300
ADPSSO CODE 70600
ADPSSO CODE 70700
ADPSSO CODE 70800
ADPSSO CODE RECYCL
ADPSSO CODE MARKET
ADPSSO CODE CDC
ADPSSO CODE 50600
ADPSSO CODE 50700
4122 4132 4200
4630 4400 4530
4540 4610 4620
4700 4714 4715
4723 4740 4800
4900 4930 NASH
ADPSSO CODE 20100
ADPSSO CODE 80000
ADPSSO CODE 70900
ADPSSO CODE ADMIN
ADPSSO CODE ADMIN
ADPSSO CODE ADMIN
ADPSSO CODE 50350
ADPSSO CODE SELF H
ADPSSO CODE 20300
NETWORK SECURITY OFFICER (NSO) AIS
ADPSSO CODE CRAFT
ALL END USERS

AUTOMATED INFORMATION SYSTEMS (AIS) SECURITY CHECKLIST

___ Power surge protectors are used on all AIS hardware.

___ Systems are located away from steam/water pipes.

___ An approved fire extinguisher is located within 75-100 each AIS.

___ Systems are clean at all times.

___ Eating, drinking or smoking is not permitted while operating systems.

___ Systems exposed to excessive dust or ather contaminants have protective covers when not in use.

___ Data diskettes are backed up at regular intervals.

___ Copyrighted software is utilized per the licensing agreement.

___ Backup disks are stored separately from originals.

___ All software is locked up when not in use.

___ A source of consumable supplies is readily available.

___ A backup system is identified (Contingency Plan).

___ AIS equipment is not moved from assigned locations without first notifying the responsible ADP System Security Officer.

___ The office space housing equipment is secured outside of normal working hours.

___ All systems are located in a securable room, or secured directly to a desk or table surface with a cable lock set.

___ All systems are secured when not in use.

___ A list of authorized users is posted.

___ Unauthorized users are not permitted to use AIS systems.

___ Log-in ID's, passwords and dial-up phone numbers are protected.

___ Classified data is processed on authorized systems only.

___ Sensitive data is protected.

___ Unattended systems are logged out.

___ No data remains on screen after logging out.

___ Disks, ribbons and output from classified processing are adequately protected or disposed of.